A PARALLEL PREVENTION ALGORITHM FOR BLACK HOLE ATTACKS IN MANET

Abdul Razak Yaakub[1], and Khalil I. Ghathwan[2,3]

[1,2]*Universiti Utara Malaysia, Malaysia, ary321@uum.edu.my*
[3]*University of Technology, Baghdad, Iraq, k.i.ghathwan@gmail.com*

ABSTRACT. In this paper, we propose a parallel algorithm for MANETs that optimizes both routing discovery and security in an Ad Hoc On-Demand Distance Vector (AODV). The new algorithm, termed as Parallel Grid Optimization by the Daddy Long-Legs Algorithm (PGO-DLLA), simulates the behavior of the biological spiders known as daddy long-legs spiders. Experiments were conducted on an NS2 simulator to demonstrate the efficiency and robustness of the proposed algorithm. The results indicate better performance than the AntNet algorithm with respect to all metrics that used in experiments such as packet delivery ratio (PDR), end-to-end delay (EtoE) and Packet loss (PL) except throughput, for which AntNet is the better algorithm. In addition, the results show that PGO-DLLA outperforms the standard AODV algorithm in simulations of both a peaceful environment and a hostile environment represented by a black hole attacks.

Keywords: mobile ad hoc networks (MANETs), black hole attack, nature inspired algorithm, secure routing

INTRODUCTION

A MANET contains many varieties of dynamic nodes. The network can be active in an actual environment without any infrastructure (Tseng, Chou, & Chao, 2011). MANETs have numerous implementations in several fields, including emergency operations, military operations, civilian environments, and personal area networking (Burbank, Chimento, Haberman, & Kasch, 2006). However, they suffer from several limitations, such as short battery lives, limited capacities, and vulnerability to malicious behaviors. A black hole is one type of attack that occurs in MANETs. Black hole nodes attack routing protocols such as the AODV protocol (Perkins & Royer, 1999), causing network packets to be dropped. The main goal of the AODV protocol is to find a path from a source to its destination node and then to forward the packets. The routing mechanism in AODV uses route requests (RREQs; for discovering routes) and route replies (RREPs; for receiving paths). However, this mechanism is vulnerable to attacks by malicious black hole nodes that can easily adjust the values of routing table fields such as *hop count* and *DSN* in order to deceive the source node after sending a RREQ, a source node will respond to the first RREP it receives. This RREP may be from a black hole node, and the source will not reply to other intermediate nodes. As a result, the cooperative work in the MANET may terminate (Tseng et al., 2011;Tamilselvan & Sankaranarayanan, 2008; Nakayama & Kurosawa, 2009; Kurosawa, Nakayama, Kato, Jamalipour, & Nemoto, 2007; Zhang, Sekiya, & Wakahara, 2009; Zhang & Lee, 2000).

Intensive computations are required to make AODV secure against black hole attacks (Mitchell & Chen, 2014). Most of the proposed solutions with limited computations such as trusting neighboring nodes, using cross-layer cooperation, or allowing route redundancy are fail to detect cooperative black hole attacks (Tamilselvan & Sankaranarayanan, 2008; Kurosawa et al., 2007; Zhang et al., 2009). However, use of intensive computations as a solution to cooperative black hole attacks may lead to depletion of the limited energy of batteries. In this paper, we develop methods to find the shortest secure path and reduce overhead using the information that is available in the routing tables (Ghathwan, Yaakub, & Budiarto, 2013), (Ghathwan & Yaakub, 2014). However, we use this information as input to propose a more complex algorithm using swarm intelligence. Mathematical formulas such as Hooke's law (Horibe, 2011) and, Newton's second and third laws (Benjamin, 2007) are utilized to evaluate the route reply and choose the best path. For example, the vibration between two nodes, depending on Hooke's low.

The remainder of this paper is organized as follows the next section discusses some related work, section for presents the proposed approach and methodology, and section for presents the solution scenarios and parameters. Finally, section for presents the conclusions.

RELATED WORK

According to Tamilselvan and Sankaranarayanan (2008), an anti-cooperative solution to black hole attacks that modified the standard AODV protocol was proposed. In the modified protocol, a source node does not respond directly when it receives the first RREP, but rather waits for a specific period of time. The source node has a cache list to save all RREPs and all details about the next hop that it gathers from other nodes. It then chooses the correct path from a list of response paths after checking for a repeated next hop node, and if there are none, it chooses a random path. The new contribution of this study was the use of a "fidelity table" and assigning fidelity levels to the participating nodes. The important point in their study is that it proposes a solution for collective black hole attacks. However, this method suffers from an increase in the control overhead, because of the exchanges of fidelity packets to achieve security.

A dynamic anomaly training method, which is one of the learning methods in data mining, was used (Nakayama & Kurosawa, 2009). The authors create a database that contains the features that result from attacks to compare these with a regular network status. They use statistical theory to produce an anomaly threshold by measuring a projection distance. This method can detect black holes in AODV with low overhead, but false positives are a major drawback of this proposal.

The Kurosawa et al. (2007) suggested a method based on the fact that attackers rely on changing the destination sequence number to the maximum number and will therefore acquire the routing and drop the packets.

PROPOSED APPROACH AND METHODOLOGY

In this paper, we propose a new mechanism that works as an intelligent swarm algorithm based on the VDLLA algorithm, which is integrated into the AODV routing protocol. The new technique, which is intended to enhance security in the AODV protocol, is called Parallel Grid Optimization by the Daddy Long-Legs Algorithm (PGO-DLLA). It tries to reduce financial and technical constraints by reducing the number of hops in the route discovery for finding the destination. This algorithm is proposed in order to reduce the severity of black hole attacks and eliminate them.

Virtual Daddy Long-Legs Algorithm (VDLLA)

The VDLLA is a swarm of spiders. We assume that each spider has nine positions represented as a 3×3 matrix in a grid space, where eight of the positions are for the spider's eight legs and the center position is for the spider's body. Each spider evaluates the nine positions based on the objective function and determines the best location from the nine positions. The best position for each spider is then evaluated to choose a global position. The computational procedure of the VDLLA is as follows.

Step1: Generate Initial population of spider members, considering N as the total number of members.
Step 2: Generate Initial location for each body of spider members randomly, and then calculate the legs position based on body position:
Assume the body position = (X, Y), the legs position is eight direction where: from up = (X,Y+0.1), from down =(X,Y-0.1), from left =(X-0.1,Y), from right = (X+0.1,Y), from up left = (X-0.1, Y+0.1), up right =(X+0.1,Y+0.1), from down left =(X-0.1,Y-0.1) and downright =(X-0.1, Y-0.1)
Step 3: Evaluate the fitness for each agent (spider) where the evaluation includes all position of agent (body + legs).
Step 4: Select the best fitness for each agent (spider) and save the position as best position.
Step 5: Select the global fitness from all best fitness and save the position as global position.
Step 6: Do while global fitness greater than tolerance value (tolerance value is based on objective function).
Step7: Find new position for each agent where the body move to best position and legs position change based on body.
Step 8: Find new best fitness and new global fitness.
Step 9: If new global fitness less than global fitness.
Step 10: Global fitness = new global fitness.
Step 11: Else if new global equal global fitness
Step 12: Change the global position using Eq. (1) below:

$$Gpos_{new} = Gpos_{old} + 0.01(RND(1,d)) \quad (1)$$

Where, d is the dimension of objective function.
Step 13: iteration=iteration +1
Step 14: End while.

Problem Formulation and Solution Representation

Aggregative conduct or swarm behavior in animals or insects is intelligent behavior of their biological group. The study of swarm intelligence is aimed at understanding the behavior of a group in nature. Biological scientists have found that many models can mimic the living systems of animals or insects.

Most spiders do not live in communities, so swarm intelligence does not reflect the collective behavior directly: rather, in this research we consider the sensitive behavior of spider legs to represent the collective performance. This approach is a relatively new orientation in the area of swarm intelligence. It is very important to develop new frameworks, which may be very useful in highly dynamic routing networks, in this area. We apply the new algorithm to MANETs, to address the problem of black hole attacks in the AODV routing protocol. The new proposal is based on the daddy long-legs spider's behavior in nature, as described in the next section.

The Propose PGO-DLLA Algorithm

In AODV routing protocol, each node has a routing table which includes the information such as; hop count, destination sequence number (DSN), life time, source IP address. PGO-DLLA have three routing tables; the first table (L1) contains a source sequence number (SSN), destination sequence number (DSN) and lifetime of the leg (LTL1). The second table (L2) contains SSN, DSN, and the force (F). The third table is the routing table that contains all a routes discovery (RD), current route discovery (CRD), life time (LT), and the best route (BR) to destination node.

The spider sends an agent (L1), to neighboring nodes to discover the route to the destination (prey). After broadcasting legs to all neighbor nodes, the spider (source) waits for a lifetime (LT) for receive (L2), if source receives L2 that means this node have a route to the destination or it is a destination. Then, the source node evaluates all route reply that comes from neighboring nodes using Eq. (2), to find the best move and select the next path. The Newton second law is computed the force. According to (Lucas, Cooke, & Friis, 1999) Newton second law is stated as "The vector sum of the forces on an object is equal to the total mass of that object multiplied by the acceleration of the object". Eq. (2) shows the original Newton second law.

$$F_{net} = ma \tag{2}$$

Where, m is the mass, a is the acceleration where can be calculated also by Newton second law Eq. (3).

$$a = \left(F_{net} / m\right) \tag{3}$$

Depending on Hook's law (Horibe, 2011) that is stated "The force exerted by the spring which is proportional to the length of stretch or compression of the spring and opposite in direction to the direction of the stretch or the compression". Eq. (4) shows the original Hook's law.

$$F = -kx \tag{4}$$

Where : K is constant, X is displacement. By replace the Eq. (3) by Eq. (4) we get the acceleration equal to Eq. (5).

$$a = -\left(\frac{k}{m}\right)x \tag{5}$$

We suppose that m equals to DSN, and K is constant number which sets 0.1.

Solution Representation

The PGO-DLLA algorithm has one main goal (shortest secure path). The main goal can be achieved by using objective function that includes two sub goal; shortest path and secure path. The Shortest Secure path in PGO-DLLA from source to destination can be calculated by the following process:

Step1: Distribute one agent to every node that is a central station to its neighbors, and this is done by checking the table of each node separately.
Step2: For each agent simultaneously (applied at same time).
Step3: Create two tables for each agent
  a) The distances table which represented the distance between agent and neighbor nodes.

b) The acceleration table which represented the evaluation function for agent to choose best path.

Step4: Find the result of evaluation function for agent using Eq. (6).

$$\alpha = \frac{kx}{m} \tag{6}$$

Step5: Create an ascending table for the (α) values (*ListMin*).

Step6: Calculated the value of threshold as Eq. (7).

$$Th_{Dynamic} = \frac{kx}{DSN(6\%)} \tag{7}$$

Step7: For ListMin (node)
If ListMin (node) <= $Th_{Dynamic}$
select Path
Exit For
else
delete Path from routing table

Step8: Next For (new node)

Step9: Stop

SOLUTION SCENARIOS AND PARAMETERS

We used the NS2 simulator, version 2.33 (Bright, Waas, King, & Cuming, 2004), to conduct simulation scenarios in order to determine the efficacy and accuracy of our AODV routing protocol. The traffic sources have a continuous bit rate (CBR). The mobility model is the random waypoint model. The map area uses a square 800×800 field with 50 nodes. The pause time varies (between 10 and 100 sec.). The simulations were run 40 times for each scenario (1–4).

Experimental Results

Simulation 1 tests the original AODV, simulation 2 tests the black hole AODV, simulation 3 tests the AntNet algorithm (Di Caro & Dorigo, 1998), (Huang, Xie, Guo, & Chen, 2012), and simulation 4 tests the proposed PGO-DLLA for discovering the shortest secure path.

Performance Metrics

Four performance indicators are used to measure the performance of the proposed PGO-DLLA, the standard AODV, the black hole AODV (BAODV) and AntNet. The details of these performance metrics are as follows:

The packet delivery ratio (PDR) is the percentage of data packets sent by the source that are received by the destination. A larger packet delivery ratio indicates better protocol performance.

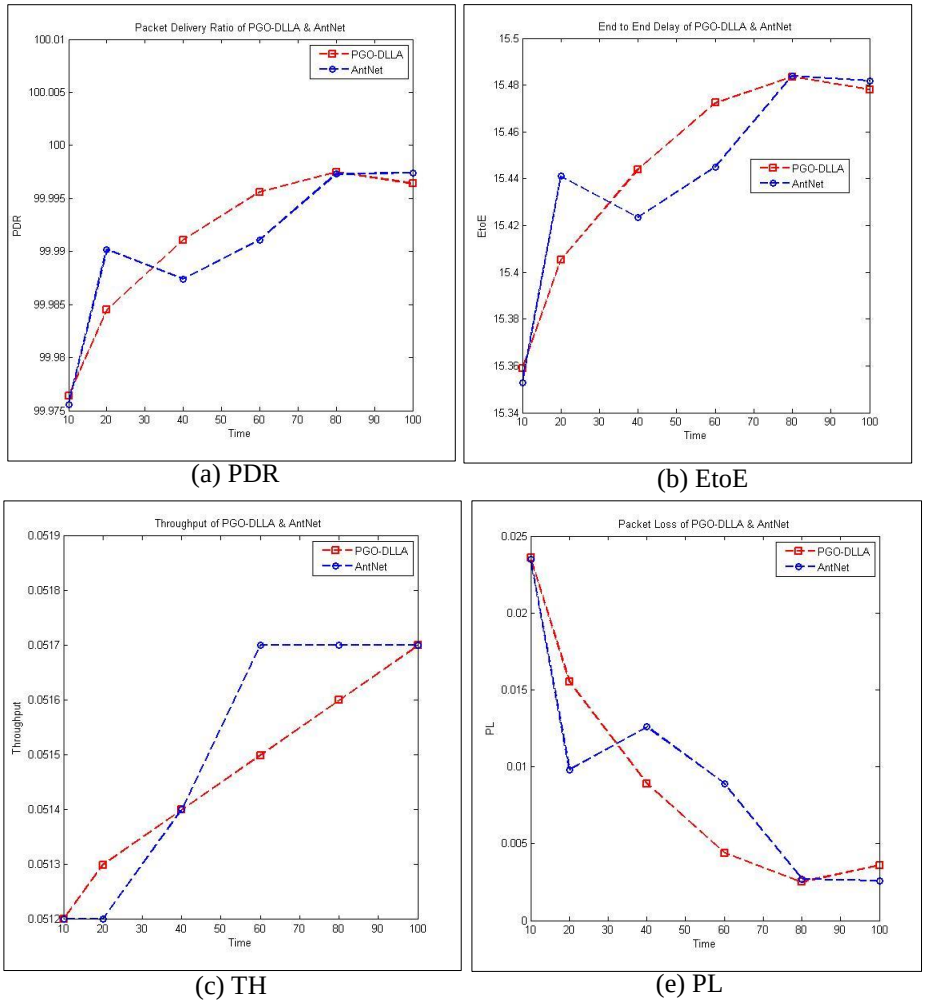
Packet loss (PL) is the percentage of packets that are lost during the simulation. A lower packet loss rate indicates better protocol performance.

The end-to-end delay (EtoE) is the average time taken for data packets to reach the destination. Only the data packets that are successfully addressed and delivered are counted. A lower end- to-end delay indicates better performance.

Throughput (TH) is the number of packets received per unit of simulation time. A higher throughput value indicates better protocol performance.

Results of the Comparison of PGO-DLLA with AntNet and Discussion

For these scenarios, the pause time was varied from 0 to 100 sec. In Figure 1-a, the PDR for PGO-DLLA was better than the PDR for the AntNet algorithm for most sets of pause times. This is because of the new routing characteristics of the proposed algorithm, which finds the shortest route to the destination node with the smallest number of hops.



(a) PDR (b) EtoE

(c) TH (e) PL

Figure 1. The Results of Comparison PGO-DLLA with AntNet

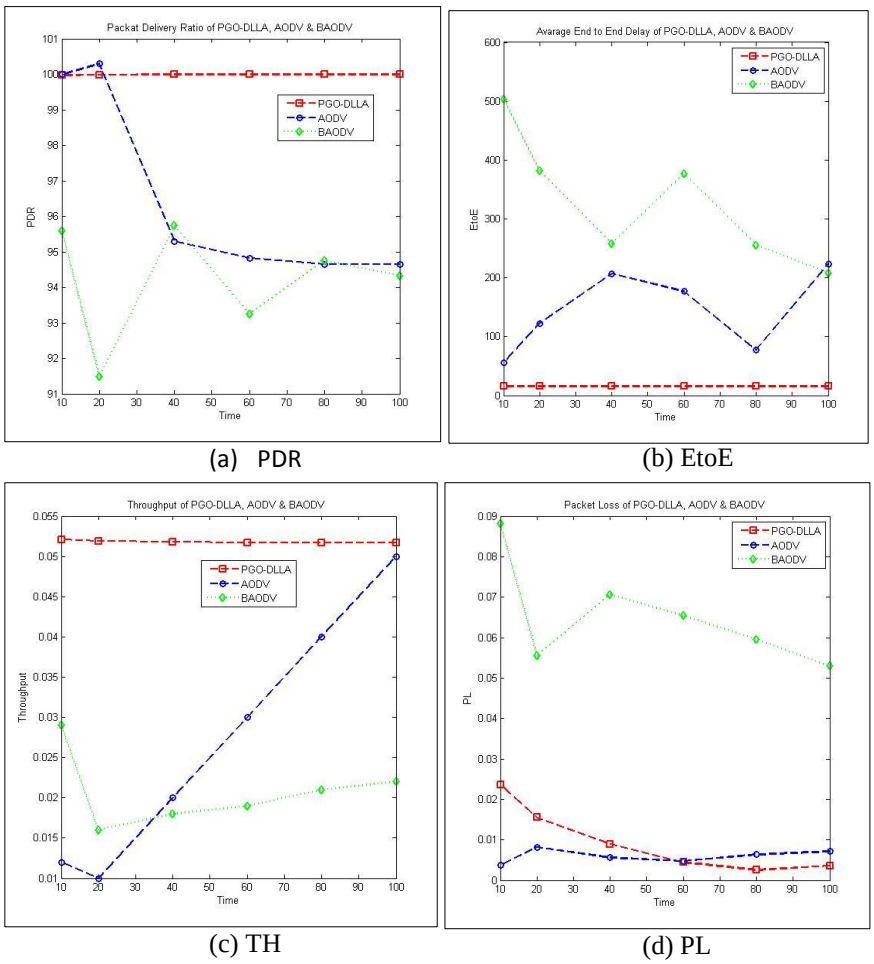
Generally, when the algorithm selects a route based on a smaller hop count, it chooses the shortest path to the destination node and thus avoids some potential link failures. For this reason, the average end-to-end delay may decrease (Sarr, Guérin-Lassous, & others, 2007). In Figure 1-b, the value of the EtoE for PGO-DLLA was slightly higher than for the AntNet algorithm. One reason for this is the calculation that is required to find a new route in order to avoid attacks. Throughput measures the number of packets from the source that are received by the destination node. If any delay occurs as the result of complex routing or updating the route, the throughput will be decreased (Li, Fang, & Li, 2010).

As shown in Figure 1-c, PGO-DLLA has better throughput than the AntNet algorithm during the first four time periods (t = 10, 20, 30,40), and, the throughput of the AntNet algorithm then becomes better. Nevertheless, the throughput of PGO-DLLA and the AntNet algorithm both increase across time. In some cases where intermediate nodes make routing decisions,

such as in self-adaptive algorithms, the nodes update the routing after each iteration. In such algorithms, the routing discovery is not done by the source node, and most of these algorithms are designed to work in dynamic environments. As a result, the packet dropping rate will increase, which results in an increased packet loss rate. However, PGO-DLLA has a more stable packet loss rate than the AntNet algorithm because of its special way of routing to the destination node, as shown in Figure 1-d.

Results of the Comparison of PGO-DLLA with AODV and BAODV and Discussion

Even though the rate of throughput is small, because the pause time equals zero (continuous motion), the PDR may be not affected (Tiong & Jassim, 2012). In such a situation, the new proposed algorithm has more than one strategy to ensure that all packets are received by the destination nodes. In Figure 2-a, we can see some decrease in the PDR for BADOV and standard AODV, as the effect of black hole attacks from a malicious node. In contrast, the PDR rate for PGO-DLLA increases, because of its strategy to avoid black hole attacks while retaining the shortest path to the destination node.



(a) PDR (b) EtoE

(c) TH (d) PL

Figure 2. The Results of the Comparison of PGO-DLLA with AODV and BAODV

Figure 2-b shows a comparison of PGO-DLLA, BADOV, and standard AODV with respect to the average end-to-end delay. In this figure we can see that PGO-DLLA has a lower rate of delay, which is because of its strategy to change the route when it is broken as a result

of misbehaving nodes. In contrast, the average end-to-end delay for BADOV increases, as the effect of black hole attacks.

Figure 2-c shows a comparison of PGO-DLLA, BADOV, and standard AODV with respect to throughput. In this figure, we can see that PGO-DLLA has a higher throughput, because it can avoid dropping packets as a result of black hole attacks and change the route to the destination if it finds any disconnection. In contrast, the throughput for BADOV is very low, which is the effect of having black hole attacks without any strategy to avoid the attacks.

Figure 2-d shows a comparison of PGO-DLLA, BADOV, and standard AODV with respect to the rate of packet loss. In this figure, we can see that BADOV has a higher loss rate, as the result of black hole attacks. In contrast, PGO-DLLA has a very low loss rate, which is very close to that of the standard AODV.

There is some improvement in the performance rate of PGO-DLLA that results from avoiding any black hole attacks and finding a shortest secure path to the destination with fewer hops.

CONCLUSION

This paper proposes a defense mechanism against a cooperative black hole attack in a MANET that relies on the AODV routing protocol. The new method is called the PGO-DLLA protocol, modifies the standard AODV and optimizes the routing process. The idea inspired by a spider called daddy long-legs is a new technique for finding suspicious nodes and avoiding black hole attacks. As a swarm algorithm, the PGO-DLLA can consolidate the routing mechanism. Some changes are made in the routing tables to store the shortest and secure path from source to destination node. The main objective in this method is to avoid black hole attacks without causing delays in the routing protocol. The experimental results show that PGO-DLLA is able to improve the performance of the network with respect to most of the performance metrics examined. For future work, we plan to examine the enforcement of additional complex attacks and the latest routing.

REFERENCES

Benjamin, C. (2007). *Laser-Tissue Interactions* (p. 218). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-540-72192-5

Bright, A., Waas, J. R., King, C. M., & Cuming, P. D. (2004). Bill colour and correlates of male quality in blackbirds: An analysis using canonical ordination. *Behavioural Processes*, *65*, 123–132. doi:10.1016/j.beproc.2003.08.003

Burbank, J., Chimento, P., Haberman, B., & Kasch, W. (2006). Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology. *IEEE Communications Magazine*, *44*(11), 39–45. doi:10.1109/COM-M.2006.248156

Di Caro, G., & Dorigo, M. (1998). AntNet: Distributed Stigmergetic Control for Communications Networks. *Journal of Artificial Intelligence Research*, *9*, 317–365. doi:10.1613/jair.530

Ghathwan, K. I., & Yaakub, A. R. B. (2014). An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET. In *Recent Advances on Soft Computing and Data Mining* (pp. 121–131). Springer International Publishing.

Ghathwan, K. I., Yaakub, A. R., & Budiarto, R. (2013). EAODV: A*-Based enhancement ad-hoc on demand vector protocol prevent black hole attacks. *Jurnal Ilmu Komputer Dan Informasi*, *6*(2), 45–51. Retrieved from http://jiki.cs.ui.ac.id/index.php/jiki/article/viewArticle/222

Horibe, S. (2011). Robert Hooke, Hooke's Law & the Watch Spring. Retrieved from http://www1.umn.edu/ships/modules/phys/hooke/hooke.htm

Huang, H., Xie, H.-B., Guo, J.-Y., & Chen, H.-J. (2012). Ant colony optimization-based feature selection method for surface electromyography signals classification. *Computers in Biology and Medicine*, *42*(1), 30–8. doi:10.1016/j.compbiomed.2011.10.004

Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile Ad Hoc networks by dynamic learning method. *International Journal of Network Security*, *5*(3), 338–346.

Li, P., Fang, Y., & Li, J. (2010). Throughput, delay, and mobility in wireless ad hoc networks. In *Proceedings IEEE INFOCOM*, 1–9.

Lucas, G. L., Cooke, F. W., & Friis, E. A. (1999). *A Primer of Biomechanics*. New York, NY: Springer New York. doi:10.1007/978-1-4419-8487-6

Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection in wireless network applications. *Computer Communications*, *42*, 1–23. doi:10.1016/j.comcom.2014.01.012

Nakayama, H., & Kurosawa, S. (2009). A dynamic anomaly detection scheme for AODV-based mobile ad hoc networks. *IEEE Transactions on Vehicular Technology*, *58*(5), 2471–2481.

Perkins, C., & Royer, E. (1999). Ad-hoc on-demand distance vector routing. In *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, 90–100. IEEE. doi:10.1109/MCSA.1999.749281

Sarr, C., Guérin-Lassous, I., & others. (2007). Estimating average end-to-end delays in IEEE 802.11 multihop wireless networks.

Tamilselvan, L., & Sankaranarayanan, V. (2008). Prevention of Co-operative Black Hole Attack in MANET. *Journal of Networks*, *3*(5), 13–20. doi:10.4304/jnw.3.5.13-20

Tiong, S. K., & Jassim, H. S. (2012). EMNet: Electromagnetic-like Mechanism based routing protocol for Mobile ad hoc network. *Trendas in Applied Sciences Research*, *7*(11), 881–900. doi:10.3923/tasr.2012.881.900

Tseng, F.-H., Chou, L.-D., & Chao, H.-C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. *Human-Centric Computing and Information Sciences*, *1*(1), 4. doi:10.1186/2192-1962-1-4

Zhang, X., Sekiya, Y., & Wakahara, Y. (2009). Proposal of a method to detect black hole attack in MANET. In *Proceedings of the International Symposium on Autonomous Decentralized Systems*, 149–154.

Zhang, Y., & Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, 275–283. New York, New York, USA: ACM Press. doi:10.1145/345910.345958